INFORMATION SECURITY POLICY

Purpose

Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Information may be put at risk by poor education and training, and the breach of security controls. Information security incidents can give rise to embarrassment, financial loss, non-compliance with legislative standards as possible legal judgements. This Information Security Policy sits alongside the Data Privacy Policy to provide an outline of the ErgoPro risk-based information security controls.

Security Objectives

- Information risks are identified, managed and treated according to an agreed risk tolerance
- Authorised users can securely access and share information in order to perform their roles
- Physical, procedural and technical controls balance user experience and security
- Contractual and legal obligations relating to information security are met
- Products consider information security at all stages of design and production
- Individuals accessing our information are aware of their information security responsibilities
- Incidents affecting our information assets are resolved and learning points taken forward to improve our controls.

Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used by us, in all formats. This includes information processed by other organisations in their dealings with us.

The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to our information and technologies, including external parties that provide information processing services, for example our data centre provider.

Detailed information about users, information assets and information processing systems is available in the ErgoPro documentation.

Compliance

Compliance with the controls in this policy will be monitored by the Information Security team and reported to the Information Governance Board.

Review

A review of this policy will be undertaken annually or more frequently as required, and will be approved by the company directors.

Policy Statement

It is our policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals
- Integrity – the accuracy and completeness of information will be maintained
- Availability – information will be accessible to authorised users and processes when required

We operate a risk-based approach to the application of controls:

- Information Security Policies
- Organisation of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity Management

Compliance

1. Information Security Policies

A set of lower level controls, processes and procedures for information security will be defined, in support of the high-level Information Security Policy and its stated objectives. This suite of supporting documentation will be approved by the directors, published, and communicated to users, partners and customers.

2. Organisation of Information Security

We will define and implement suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security within the business.

3. Human Resources Security

Our security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training will be made available to all staff, and poor and inappropriate behaviour will be addressed. Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

4. Asset Management

All assets (information, software, electronic information processing equipment, service utilities and people) will be documented and accounted for. Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets. All information assets will be classified according to their legal requirements, business value, criticality and sensitivity, and classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

5. Access Control

Access to all information will be controlled and will be driven by business requirements. Access will be granted, or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties. A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed and will include consideration of multiple factors as appropriate. Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

6. Cryptography

Our systems use the latest methods for encrypting data, including the hashing and salting of sensitive data such as passwords stored in database systems. Data transmitted will be encrypted using the latest protocols and methods.

7. Physical and Environmental Security

Information processing facilities are housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack.

8. Operations Security

We will ensure the correct and secure operations of information processing systems.

This will include:

- Documented operating procedures
- The use of formal change and capacity management
- Controls against malware
- Defined use of logging
- Vulnerability management

9. Communications Security

We will maintain network security controls to ensure the protection of information within its networks, and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information.

10. System Acquisition, Development and Maintenance

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems. Controls to mitigate any risks identified will be implemented where appropriate. Systems development will be subject to change control and separation of test, development and operational environments.

11. Supplier Relationships

Our information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected. Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

12. Information Security Incident Management

Guidance will be available on what constitutes an Information Security incident and how this should be reported Actual or suspected breaches of information security must be reported and will be investigated Appropriate corrective action will be taken, and any learning built into controls.

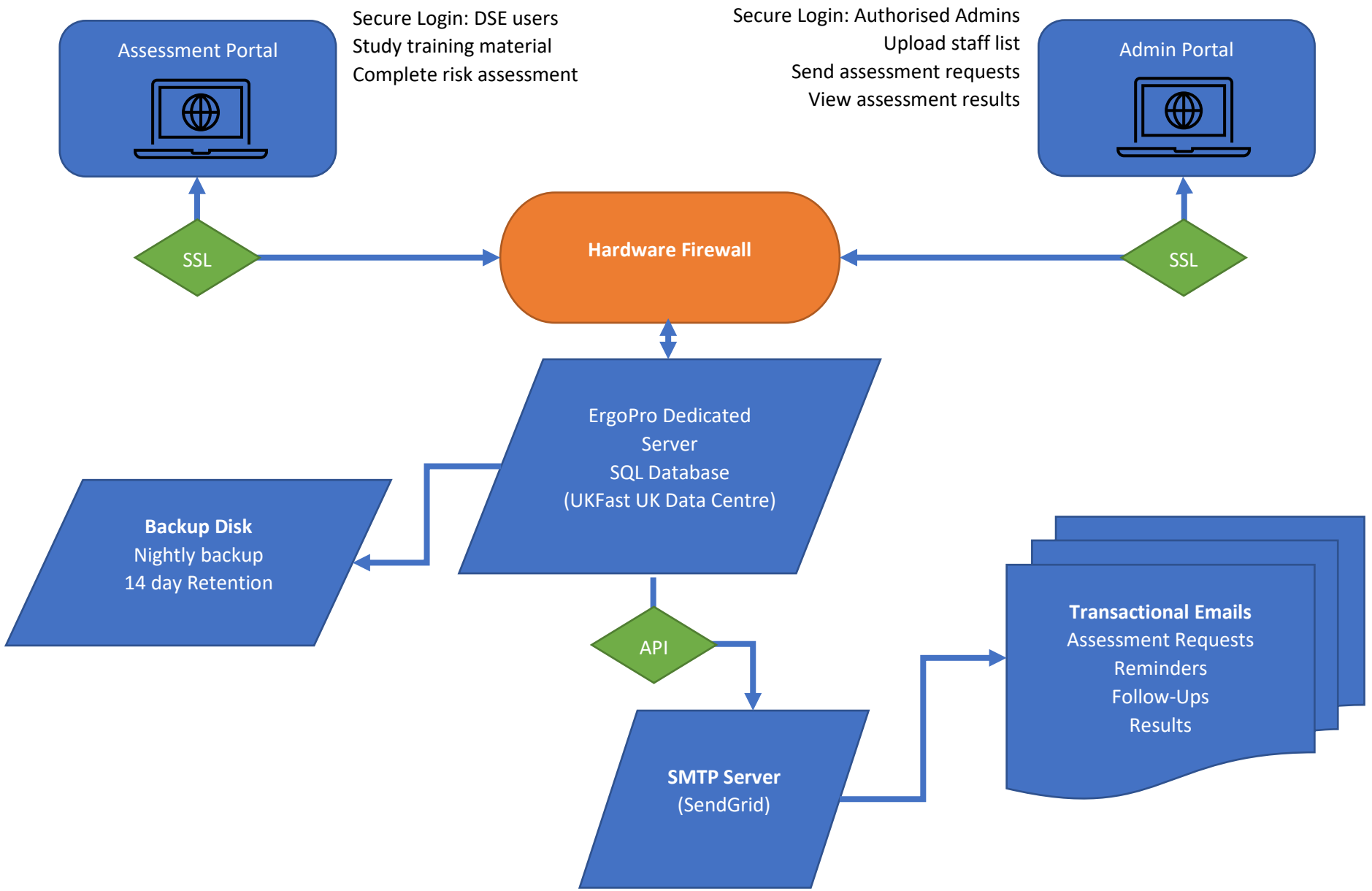
13. Information Security Aspects of Business Continuity Management

We have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely recovery in line with documented business needs. This includes appropriate backup routines and built-in resilience. Business continuity plans are maintained and tested in support of this policy. Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

14. Compliance

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements. Currently this includes data protection legislation (GDPR), payment card industry standard (PCI-DSS), the Government's Prevent guidance and our contractual commitments. We will use a combination of internal and external audit to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures. This will include IT Health Checks, vulnerability scanning, penetration testing, gap analyses against documented standards, internal checks on staff compliance, and returns from Information Asset Owners.

ErgoPro Information Flow



Certificate of Approval

This is to certify that the Management System of:

UKFast.net Limited

UKFast Campus, Birley Fields, Manchester, M15 5QJ, United Kingdom

has been approved by LRQA to the following standards:

ISO 14001:2015 | ISO 9001:2015 | ISO/IEC 27001:2013 | ISO 22301:2012

David Derrick

Issued by: Lloyd's Register Quality Assurance Limited

This certificate is valid only in association with the certificate schedule bearing the same number on which the locations applicable to this approval are listed.

Current issue date: 24 June 2019
Expiry date: 23 June 2022
Certificate identity number: 10195623

Original approval(s):
ISO 14001 – 6 April 2017
ISO 9001 – 6 April 2017
ISO/IEC 27001 – 6 April 2017
ISO 22301 – 27 February 2018

Approval number(s): ISO 14001 – 00009472 / ISO 9001 – 00009473 / ISO/IEC 27001 – 00009474 / ISO 22301 – 00012675

This certificate is a continuation of a previous approval from another certification body as follows:
Previous original ISO 14001 approval on 19-JAN-2011, Alcumus ISOQAR certificate number 8396-EMS - 001
Previous original ISO 9001 approval on 19-JAN-2011, Alcumus ISOQAR certificate number 8396-QMS - 001
Previous original ISO/IEC 27001 approval on 23-JUN-2010, Alcumus ISOQAR certificate number 8396-ISN - 001

The scope of this approval is applicable to:

Provision of hosting services, the consultation, design, implementation, proactive maintenance and support of bespoken client managed services and all supporting business processes provided from Manchester Head Office and data centres. Statement of Applicability version 2.n

UKAS MANAGEMENT SYSTEMS
001

Certificate Schedule

Certificate identity number: 10195623

Location	Activities
UKFast Campus, Birley Fields, Manchester, M15 5QJ, United Kingdom	ISO 14001:2015 ISO 9001:2015 ISO22301:2012 Provision of bespoken consultation and design of architecture relating to dedicated managed services, including Cloud services, provided from Manchester Head Office and data centres. ISO/IEC 27001:2013 Assessment Scope: Provision of bespoken consultation and design of architecture relating to dedicated managed services, including Cloud services, provided from Manchester Head Office and data centres. Statement of Applicability version 2.n
MANOC04, United Kingdom	ISO 14001:2015 ISO 9001:2015 ISO 22301:2012 Data Centre Services. ISO/IEC 27001:2013 Data Centre Services. Statement of Applicability version 2.n
MANOC05, United Kingdom	ISO 14001:2015 ISO 9001:2015 ISO 22301:2012 Data Centre Services. ISO/IEC 27001:2013 Data Centre Services. Statement of Applicability version 2.n
MANOC06, United Kingdom	ISO 14001:2015 ISO 9001:2012 ISO 22301:2012 Data Centre Services.

UKAS MANAGEMENT SYSTEMS
001

Certificate Schedule

Certificate identity number: 10195623

Location	Activities
	ISO/IEC 27001:2013 Data Centre Services. Statement of Applicability version 2.n
MANOC07, United Kingdom	ISO 14001:2015 ISO 9001:2015 ISO 22301:2012 Data Centre Services. ISO/IEC 27001:2013 Data Centre Services. Statement of Applicability version 2.n

UKAS MANAGEMENT SYSTEMS
001

Record of Verification/Assurance

This is to confirm that LRQA has undertaken a review and assessment including process sampling to verify that:

UKFast.net Limited

UKFast Campus, Birley Fields, Manchester, M15 5QJ, United Kingdom

has implemented the applicable requirements provided in ISO 27018:2014 and ISO 27017:2015

David Derrick

Issued by: Lloyd's Register Quality Assurance Limited

Current Issue Date: 30 May 2019

Record No: LRQ00001193

Original Statement: 01 October 2018

Statement Expiry: 29 May 2022

Scope of Activities:

Data Centre Services. Statement of Applicability version 2.n.

How does ErgoPro use your personal information?

Personal information on you is only collected when you are required to carry out a workstation assessment.

It is important to ensure that your information is kept confidential, under the terms of the General Data Protection Regulation (GDPR). We want you to know about this.

The information which you give us about yourself will be retained by us in our records.

We will only use this information to complete the process of a workstation risk assessment. You will always be given the opportunity to say that you do not wish this to happen, in which case in the first instance you should contact your line manager or HR department. Or contact is using the details shown below.

Information held by us will only be retained for as long as is necessary in relation to the workstation risk assessment. Health and safety law does not stipulate how long this information should be kept, but it is considered prudent to keep it for the same period as the legal statute of limitations allows.

You have the right to see a copy of any information we hold about you by written request. You should do this in the first instance by asking your line manager or HR department who can provide this information via the ErgoPro Admin Portal. Or you can contact us using the details shown below.

Your employer is responsible for ensuring that the personal data held by us is accurate and kept up to date.

Does ErgoPro collect other forms of information about its users?

We will gather a certain amount of anonymous information about users which does not personally identify you, but which may be helpful for statistical purposes or for improving the services we offer. For example, we will track how many users visit a certain page, and for how long, so we can measure whether the site is effective. Generally, this information is collected through "traffic data" and may entail the use of ‘Cookies’, ‘IP addresses’ or other data methods used to identify a computer.

Is my Personal Information secure from others when using ErgoPro?

Personal Information collected by ErgoPro is stored in secure operating environments that are not available to the public, or other companies. ErgoPro stores data at UK data centres operated by UKFast, a Microsoft Gold certified data hosting organisation. This provides for strict network and physical security of data and includes measured designed to prevent the loss, destruction of, or damage to your personal data.

Where will my data be kept?

Your data is stored at a UK datacentre operated by UKFast, a Microsoft Gold certified data hosting organisation. Your data will not be transferred to a country or territory outside the UK.

Does ErgoPro use Cookies?

Yes. Cookies are one method by which a computer stores information that needs to be retained across user sessions. They are stored by your web browser and allow for useful functionality such as recognising you as a user or personalisation of product and features. Cookies themselves do not personally identify you, although they do identify your web browser or computer.

Most web browsers are initially set to accept cookies, but if you prefer, you can set yours to refuse cookies. However, you may not be able to use the website or take full advantage of the functionality available.

Will my information be shared with anyone else?

Your workstation risk assessment will be available to approved persons within your employer's organisation. This is usually your line manager and HR or Health & Safety department. This is to review your workstation risk assessment for risk assessment and risk reduction purposes, to ensure your health and safety in the workplace. A workstation risk specialist approved by your employer's organisation may review your risk assessment information so that a more detailed review can be carried out. You will be notified should this be required.

How do I contact ErgoPro about my personal information?

Please address your Data Protection queries and requests to:

Data Protection Officer
ErgoPro
Ciscom Internet Ltd
85 Church Road
Hove
BN3 2BB,

Phone 01323 886205

Email: info@ergopro.co.uk